КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.4.8589
УДК 681.3(043.2)

Куліковський Антон Володимирович
здобувач рівня «Доктор філософії»
Національний авіаційний університет, Київ, Україна
OrcID 0000-0002-8641-4452
anton.kulikovskyi@gmail.com

ТЕХНОЛОГІЯ BLOCKCHAIN ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. В статті описано використання інформаційно-телекомунікаційних систем в державних і приватних установах та недоліки до побудови інформаційно-телекомунікаційних систем за принципом децентралізації. Проведено аналіз останніх досліджень та публікацій за темою блокчейн. В роботі описано принцип роботи технології блокчейн та способи, якими блокчейн захищає себе від спроб внесення несанкціонованих змін чи видалення даних. Розглянуто доцільність та перспективи використання технології блокчейн в сфері інформаційної безпеки з точки зору тріади сервісів інформаційної безпеки як конфіденційність, цілісність та доступність й зроблено висновки. Із швидким розвитком інформаційних технологій пропорційно швидко збільшується і кількість уразливостей та загроз інформаційно-телекомунікаційних систем, адже більшість цих систем побудована і працює за централізованим принципом. Перспективним напрямком для побудови інформаційно-телекомунікаційних систем є використання принципу децентралізації. Тому важливим є аналіз використання технології Blockchain для побудови децентралізованих інформаційно-телекомунікаційних систем з точки зору інформаційної безпеки.

Ключові слова: blockchain; децентралізована мережа; інформаційна безпека

ВСТУП

Сьогодні відбувається швидкий розвиток інформаційно-телекомунікаційних систем та технологій і як наслідок їх широке застосування в різних сферах діяльності суспільства. Значна кількість сучасних державних та приватних установ використовує інформаційно-телекомунікаційні системи для управління виробничими процесами, підтримки прийняття рішень, збереження та обробки інформації, пошуку необхідних даних тощо. Майже всі ці системи працюють за принципом, коли управління процесами відбувається централізовано й повний контроль над системою можна здобути отримавши доступ до головного центрального сервера. Внаслідок чого збільшується ризик компроментації всієї системи, кількість уразливостей та загроз ІТС.

Постановка проблеми. У зв'язку з суспільним інтересом до технології блокчейн та її активним застосуванням в різних сферах, таких як фінанси чи облік, постає доцільним провести аналіз ефективності застосування блокчейн в сфері інформаційної безпеки

Аналіз останніх досліджень і публікацій. Перша робота над ланцюгом блоків, що захищений криптографічними функціями була описана 1991-го року Стюартом Хабером та У. Скоттом Сторнеттою. Вони хотіли запровадити систему, в якій часові позначки документів неможливо спотворити чи пошкодити. 1992-го року Байєр, Хабер і Сторнетта використали в проекті дерево Меркла, що покращило ефективність, дозволяючи включати в один блок декілька документів.

ISSN 2663 - 4023

Перший варіант блокчейну було розроблено людиною (або групою людей), відомою як Сатоші Накамото 2008-го року. Такий підхід до організації роботи розподіленого реєстру Накамото втілив 2009 року, розробивши основний складник криптовалюти Bitcoin, де він виступає в ролі відкритої книги обліку для всіх транзакцій мережі[1].

У 2015 році в журналі The Economist було опубліковано статтю «Машина довіри», в якій описана можливість повної зміни економіки за допомогою блокчейн. Оскільки саме ця технологія стала першою, яка змогла вирішити проблему довіри між сторонами без залучення третіх осіб та посередників[2].

Мета статті. Метою статті є аналіз ефективності використання технології блокчейн в сфері інформаційної безпеки.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Термін Blockchain своєю назвою частково характерезує принцип роботи самої технології. «Block» - це блок, «chain» - це ланцюжок. З чого слідує, що Blockchain це ланцюжок блоків. Але не просто ланцюжок. В ньому витримана строга послідовність визначена складними криптографічними функціями.

Блоки – це дані про транзакції, угоди та контракти всередині системи представлені у криптографічній формі. Всі блоки вибудувані в ланцюжок, тобто послідовно пов’язані між собою. Для додавання(запису) нового блоку необхідна перевірка послідовності попередніх блоків.

Розглянемо роботу Blockchain більш розгорнуто. Кожен блок або запис в реєстрі Blockchain містить основну інформацію, розрахований власний хеш та хеш попереднього блоку. Набір даних, що зберігаються всередині блоку залежать від цільового призначення Blockchain. Наприклад Blockchain біткоїн містить інформацію про відправника, одержувача та кількість перерахованих монет. Хеш кожного блоку буде унікальним, як і дані, що зберігаються всередині блоку. Його унікальність можна порівняти з відбитком пальця людини. Внесення будь-яких змін в блок одразу спричинить зміну хешу блока. Третім елементом блоку є хеш попереднього блоку. Таким чином формується послідовність блоків. Така модель робить Blockchain безпечним.

Розглянемо приклад. На рисунку 1 зображено послідовність з трьох блоків.

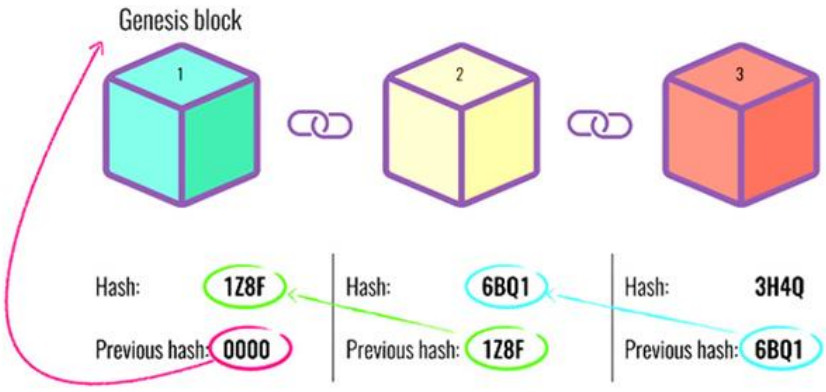

Рис. 1. Послідовність блоків

ISSN 2663 - 4023

Кожен блок має свій хеш та хеш попереднього блоку. Блок 3 вказує на блок 2, блок 2 на блок 1. Перший блок особливий, він не може вказати на попередній блок, оскільки такого не існує, цей блок називається genesis блок.

Спробуємо порушити цілісність та несанкціоновано внести зміни в блок 2. Зміна навіть одного симоволу в даних блоку 2 призведе до зміни його хешу, що автоматично призведе до змін у всіх наступних блоках і зробить їх недійсними. Але використання самого хешування для запобігання створення підроблених блоків недостатньо.

Обчислювальні машини сьогодні мають великі потужності та можуть розрахувати тисячі хешів в секунду. Тому існує велика ймовірність підробити блок та перерахувати всі наступні блоки, щоб зробити блокчейн знову дійсним.

Для попередження таких випадків в блокчейн є алгоритм Proof of Work. Його суть полягає в пошуку хеш функції, результат якої починається з певної кількості нулів. Цей механізм сповільнює створення нових блоків та захищає від DDoS атак. У випадку з біткоїн потрібно близько 10 хвилин для розрахунку нового блоку та додавання його в загальну послідовність блоків мережі. Proof of Work значно ускладнює можливість підробки блоків, оскільки підробивши один блок, всі наступні блоки також необхідно перерахувати через Proof of Work. Спільне використання цього механізму разом з хешами блоків складає основу безпеки Blockchain.

Є ще один спосіб, яким Blockchain захищає себе і це децентралізація. Замість використання централізованого об’єкту для управління всією послідовністю, кожен вузол має свою копію реєстру та використовує однорангову мережу для зв’язку з іншими вузлами. Будь-хто може приєднатись до мережі, отримати повну копію реєстру та приймати участь в перевірці валідності послідовності блоків. Після створення нового блоку він відправляється всім підключеним до мережі вузлам для перевірки хешу (справжності блоку). Якщо перевірку пройдено, кожен вузол додає новий блок в свою копію Blockchain. Всі вузли досягають консенсусу, погоджуючись з тим, які блоки валідні, а які ні. Фальсифіковані блоки будуть відхилені іншими вузлами мережі. Тому, щоб успішно фальсифікувати блок в блокчейн, необхідно перерахувати його хеш та хеш всіх наступних блоків через алгоритм Proof of Work, а також мати доступ більш як до 50% вузлів мережі, що практично неможливо.

За принципом своєї роботи Blockchain володіє такими перевагами як:

• Децентралізація. Відсутній головний сервер зберігання даних. Всі записи зберігаються у кожного учасника мережі.

• Прозорість роботи. Будь-хто з учасників може перевірити всі транзакції, що проходять в системі

• Безпечність. Всі операції надійно захищені криптографічними функціями

• Надійність. Будь-яка спроба внести несанкціоновані зміни буде відхилена іншими учасниками мережі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Мережа блокчейн добре справляється із забезпеченням збереження цілісності даних. За рахунок існування багатьох копій бази даних та внесення змін до неї лише після підтвердження правильності інформації іншими учасниками мережі, інформація залишається захищеною від навмисної, несанкціонованої або випадкової зміни, а також будь-яких змін в процесі зберігання обробки або передачі. Інформацію стає неможливо змінити через технічні збої в роботі вузла мережі або через людський фактор, оскільки

підтвердження операцій відбувається завдяки складним математичним функціям. Як наслідок інформація залишається незмінною та коректною. Забезпечення цієї категорії інформаційної безпеки дає можливість стабільного проведення операцій, прийняття правильних рішень та можливість зберегти дані в тому вигляді, в якому вони були створені.

Відповідно до принципу доступності інформація має бути доступною авторизованим особам в потрібний момент часу. В мережі блокчейн кожен учасник вважається авторизованим та в будь-який момент може зчитати чи записати дані та приймати участь у верифікації даних, які додають інші учасники.

Конфіденційність інформації досягається наданням можливості доступу до неї з найменшими привілеями, тобто авторизована особа повинна мати доступ тільки до тих даних, які визначені для неї правами доступу. Кожен учасник мережі може отримати повну копію бази даних на свій пристрій та прочитати в ній всі дані, що в основі суперечить принципу конфіденційності даних. Зберігання даних в блокчейн в зашифрованому вигляді в основі не вирішить проблему конфіденційності, оскільки в більшості випадків конфіденційні дані з часом не втрачають своєї актуальності, як, наприклад, персональні дані. А розшифрування отриманих даних стає питанням часу та залежить від обчислювальних потужностей зловмисника, який намагається отримати доступ до інформації.

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В результаті проведеного аналізу можна зробити висновок, що за принципом своєї роботи блокчейн з високою надійністю можна використовувати для побудови інформаційно-телекомунікаційних систем, які призначені для обробки та збереження відкритих даних з метою забезпечення їх цілісності та доступності. Використовувати блокчейн в загальному вигляді для зберігання та обробки конфіденційних даних не є доцільним, оскільки будь-хто зможе отримати доступ до конфіденційних даних, які зберігаються у відкритій базі блокчейн.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] BitFury Group. Proof of Stake vs. Proof of Work White Paper, 2015. 30 с.
[2] «The trust machine», The Economist Newspaper, 2015. Режим доступу: https://www.economist.com/leaders/2015/10/31/the-trust-machine.
[3] Інформаційна безпека, Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/Інформаційна.
[4] Джонсон Ричард, Технология распределенных регистров: что мы можем узнать из недавних атак на блокчейн, 2016.
[5] Винья Пол. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок. М.: Издательство «Манн, Иванов и Фербер», 2017.
[6] W. Mougayar, “The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology,”NewYork, USA,JohnWiley& SonsInc., 2016.
[7] «OpenMarket (ДП „СЕТАМ“)». Режим доступу: https://minjust.gov.ua/news/ministry/openmarket-dp-setam-proviv-24-tisyachi-auktsioniv-z-vikoristannyam-tehnologii-blockchain-na-mayje-700-mln-grn .

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023

Anton V. Kulikovskyi
PhD student
National Aviation University, Kyiv, Ukraine
OrcID 0000-0002-8641-4452
anton.kulikovskyi@gmail.com

BLOCKCHAIN AS A COMPONENT OF INFORMATION SECURITY

Abstract. The article describes the use of information and telecommunication systems in public and private institutions and disadvantages for the construction of information and telecommunication systems for decentralization. The analysis of recent researches and publications on the subject of the block is conducted. The paper describes the principle of the technology, the block and the ways in which a block protects itself from attempting to make unauthorized changes or deletion of data. The expediency and perspectives of using information security technologies from the point of view of the triad of information security services as confidentiality, integrity and accessibility are considered. The rapid development of information technology is expected to rapidly increase and increase, and also threatens the information and telecommunication systems that have most of these systems. A promising direction for the construction of information and telecommunication systems is the use of decentralization. Therefore, it is important to analyze the use of Blockchain technology for the construction of decentralized information and telecommunication systems in terms of information security.

Keywords blockchain; decentralized network; informational security.

REFERENCES

[1] BitFury Group. Proof of Stake vs. Proof of Work White Paper, 2015. 30 c.
[2] «The trust machine», The Economist Newspaper, 2015. Access mode: https://www.economist.com/leaders/2015/10/31/the-trust-machine.
[3] Informacijna bezpeka,Wikipedia. – Access mode: https://uk.wikipedia.org/wiki/Інформаційна.
[4] Johnson Richard. Distributed Ledger Technology: What We Can Learn from Recent Blockchain Attacks, 2016.
[5] Paul Vigna and Michael J. Casey "The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order", 2017.
[6] W. Mougayar, “The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology,”NewYork, USA,JohnWiley& SonsInc., 2016.
[7] «OpenMarket (ДП „СЕТАМ“)». Access mode: https://minjust.gov.ua/news/ministry/openmarket-dp-setam-proviv-24-tisyachi-auktsioniv-z-vikoristannyam-tehnologii-blockchain-na-mayje-700-mln-grn .